Protecting Cyberspace

The most vital systems of our society are all dependent on technology and computers. As a nation, we are only as strong as the security on the weakest link on these interconnected and interoperable systems. A weak link can allow a hacker to open a dam, close down an air traffic control system, or create financial havoc for our banking industry. We must secure these weak links by building strong prevention, detection, and response mechanisms for addressing potential threats to our networks. If cybersecurity is not a priority, then our economy and our infrastructures are at risk. Government, the private sector, and academia should all work together to develop a culture of security in cyberspace.

According to a recent survey conducted by the Pew Internet and American Life Project, almost half of Americans fear terrorists will launch cyberattacks on our critical infrastructures, disrupting major services and crippling economic activity.[1] These fears are not unwarranted; as during the past decade our critical infrastructures, military operations, business, and home networks have become interconnected and interdependent. These interdependencies, however, are neither well understood nor well mapped. In addition, our computer systems are global and connected to similar networks around the world. These connections create international challenges and underscore the need to work with other countries in securing their systems. The result of this increasing interdependency is that the threats to and vulnerabilities in our nation's cybersecurity are growing faster than we can address them.

It was only a few years ago that a computer hacker gained control of a telephone system and disabled the control tower of the Worcester, Massachusetts airport, shutting down the airport for more than six hours.[2] Others have penetrated the computer systems of the California Independent System Operator, the nonprofit corporation that controls the distribution of 75 percent of the state's electricity, and the Roosevelt Dam in Arizona.[3] In the latter case, it is believed that the intruder gained command of the system that controlled the dam's floodgates and 400 trillion gallons of water. If he had released the flood gates, there would have been widespread loss of life and damage to the towns downstream of the dam. Some communities, infrastructures, and our economy have already suffered from cyber attacks. For example, an individual gained access to a utility company computer in Australia in 2000, releasing millions of gallons of raw sewage into a Queensland community's waterways.[4] Just this past summer, the Sobig computer virus

---

[1] Pew Internet & American Life, *The Internet and Emergency Preparedness: joint survey with Federal Computer Week magazine*, August 31, 2003, http://www.pewinternet.org/reports/toc.asp?Report=100.

[2] U.S. Department of Justice, "Juvenile Computer Hacker Cuts off FAA Tower At Regional Airport - First Federal Charges Brought Against a Juvenile for Computer Crime," press release, March 18, 1998, http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm.

[3] U.S. Department of Justice, *Statement of Michael Chertoff, Assistant Attorney General, Criminal Division Before the Committee on the Judiciary, Subcommittee on Crime, U.S. House of Representatives*, June 12, 2001; *see also* Barton Gellman, "Cyber-Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *Washington Post*, June 27, 2002, Page A01.

[4] Ibid.

temporarily shut down the 23,000-mile-long CSX rail system.[5] Indeed, Sobig, along with the Blaster and Welchia viruses, caused more than $32.8 billion in economic damages in August 2003 alone, according to mi2g, a digital risk assessment company based in London.[6] The damages caused by Mydoom-A, which struck computers worldwide the week of January 26, 2004, has yet to be undetermined, though we know that by January 27 it had infected one out of every 41 e-mail messages.[7]

SECURITY GAP: We Are Not Prepared for an Electronic "9-11."

If an electronic 9-11 were to happen tomorrow, who in the government could coordinate the efforts of dozens of agencies and effectively reach out to the private sector, which owns 85 percent of our critical infrastructures? It is not clear who has the authority and capability within the federal government to bring together the various federal and state agencies, as well as the relevant private sector entities, in the event of a cyber-catastrophe.

In 1996, the United States government, recognizing the need for a comprehensive national strategy to protect cyberspace, created the first national effort to secure our networks.[8] Among the entities created as a part of this strategy were the National Infrastructure Protection Center (NIPC), a multi-agency organization housed at the FBI that served as the focal point for coordinating government-wide cybersecurity and critical infrastructure response, and the Critical Infrastructure Assurance Office (CIAO), a Commerce Department entity tasked with developing national critical infrastructure protection plans and coordinating outreach, education, and awareness programs.[9] These entities recognized the need to pool the resources of numerous agencies and engage the private sector in the country's cybersecurity efforts.

Soon after September 11, 2001, the current Administration created the Critical Infrastructure Protection Board to coordinate and oversee federal efforts to protect the networks and systems of critical infrastructures, federal assets, and national security programs.[10] The Board was comprised of senior governmental officials and chaired by Richard Clarke, who also served as special advisor to the President for cyberspace security and headed the White House Office of Cybersecurity.

Less than a year and a half after its creation, in April 2003, the Critical Infrastructure Board was dissolved. [11] NIPC and CIAO have been eliminated, with some, but not all, of their former responsibilities transferred over to the Department of Homeland Security (DHS). Clarke, his deputy, and the top officials at NIPC and CIAO left the government, leaving many wondering

---

[5] CSX Corp., "Computer Virus Strikes CSX Transportation Computers," press release, August 20, 2003, http://www.csx.com/index.cfm?fuseaction=company.news_detail&i=45722&ws=corporation.
[6] Mi2g, http://www.mi2g.com/.
[7] John Hogan, "A week of gloom and Mydoom," *searchwin2000.com*, January 30, 2004.
[8] President, "Executive Order 13010—Critical Infrastructure Protection," 61 *Fed. Reg.* 138, July 17, 1996.
[9] President, "Presidential Decision Directive 63," May 22, 1998.
[10] President, "Executive Order 13231-Critical Infrastructure Protection in the Information Age," 66 *Fed. Reg.* 53063, October 18, 2001.
[11] Diane Frank,"Tritak departs CIAO, government," *Federal Computer Week*, January 17, 2003, http://www.fcw.com/fcw/articles/2003/0113/web-tritak-01-17-03.asp; *see also* Dan Verton, "NIPC chief Ron Dick to retire," *Computerworld*, December 9, 2002, http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,76538,00.html.

who was in charge of protecting our infrastructures[12] and whether the Administration was dedicated to protecting the nation's cyber networks.[13]

Amid criticism from the private sector regarding the lack of attention being paid by the government to cybersecurity, DHS announced on June 6, 2003, the creation of the National Cyber Security Division (NCSD). With a requested budget of $80 million for Fiscal Year 2005, the NCSD is tasked with coordinating the cybersecurity activities within DHS and other agencies and is to serve as the central point of contact for the private sector.[14] It took three months for the Administration to find a director willing to lead NCSD. Concerns remain that the new director is buried too deep in the bureaucracy of DHS with little authority for effectively leading our country's cybersecurity efforts.[15] Additionally, the Director does not have the authority to direct the multiple agencies, at the senior level needed, in the event of a cyber incident.

The Administration, overall, has been moving too slowly on securing our computer networks. It has been more than a year since February 2003 when the Administration released its "National Strategy to Secure Cyberspace," which set forth five cybersecurity priority areas. Those areas included:

- The development of a cybersecurity response system;
- The creation of a threat and vulnerability reduction program;
- The creation of awareness and training programs;
- The unveiling of plans for securing government computers; and
- The development of plans detailing national security and international cooperation.

The Administration's efforts to implement the strategy are lagging, leaving our nation at risk and unprotected. Since the creation of the NCSD nine months ago, DHS has announced then eliminated cybersecurity initiatives such as the Cyber Security Tracking, Analysis, & Response Center (CSTARC), a unit designed to detect and response to Internet events, track potential threats and vulnerabilities, and coordinate incident response with federal, state, local, private sector, and international partners.

The agency also is just beginning to provide some of the services that were available in similar form prior to the reorganization that created the agency. In September 2003, DHS created the US-CERT program to aggregate available cyber security information and provide it to individuals and organizations in a timely and understandable manner. Many questions remain as to when the US CERT will be fully functioning, how it will work with the Information Sharing and Analysis Centers (ISACs) that are responsible for private sector information sharing initiatives, and how it will work with the private sector. To date, the initiatives announced by the US CERT appear to recreate, in part, programs that existed before DHS was created or duplicate private sector

---

[12] Barton Gellman, "Anti-Terror Pioneer Turns In the Badge After 11 Years, Clarke Leaves Legacy of Lasting Change -- and Enemies," *Washington Post*, Page A21, March 13, 2003; *see also* William Jackson, "Howard Schmidt is Leaving the White House," *Government Computer News*, April 21, 2003, http://www.gcn.com/vol1_no1/daily-updates/21815-1.html.

[13] "Uncertain Future for Cybersecurity? Now that PCIPB has been dissolved, Illena Armstrong questions how future initiatives will be led," *SC Magazine*, April 2003.

[14] "Tech Industry Wants Cybersecurity Czar," *Foxnews.com*, April 23, 2003, http://www.foxnews.com/story/0,2933,84865,00.html.

[15] Dan Verton, "A major DHS cybersecurity post remains vacant," *Computerworld*, July 21, 2003, http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,83242,00.html.

initiatives. These programs do not bring the nation much further on securing our computer networks than we were two years ago when NIPC, CIAO, and other entities existed.

For example, DHS announced in January that the NCSD, through US CERT, would begin producing several new "products" to inform individual computer users and security professionals about cyberthreats via e-mail. This announcement came a day after the Mydoom-A virus struck our nation's computers. These products, in part, seem to replicate initiatives that existed at NIPC. Technical users can now receive "summaries of security issues, new vulnerabilities, potential impact, patches and work-arounds" on cyber security-related issues.[16] NIPC published assessments, advisories, and alerts, including "CyberNotes," which provided security professionals "with timely information on cybervulnerabilties, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices."[17] Many cybersecurity experts also have pointed out that the alert system duplicates efforts of several private sector entities.[18]

More recently, DHS announced the creation of a Cyber Interagency Incident Management Group to bring together officials from law enforcement, national security, and defense agencies for voluntary periodic meetings at a staff level for planning responses to major cybersecurity incidents. These agencies, however, gathered together before the Department and the NCSD existed under Richard Clarke's direction to assess viruses and other computer incidents as they happened. Recreating the programs that existed two years ago simply is not enough if we are to protect our vital networks and infrastructures. More should be done to "facilitate interactions and collaborations" among the federal agencies tasked with cybersecurity responsibilities, as required by the Homeland Security Presidential Directive-7 (HSPD-7) issued in December 2003.

If DHS is to implement a successful cybersecurity agenda, it should fully engage the private sector. It has made some efforts to do so, including its participation in the National Cybersecurity Summit organized by several IT associations and entities last December. Despite these efforts, more should be done and DHS should fully consult with relevant private sector entities in developing comprehensive cybersecurity. For example, several ISACs were not consulted when DHS developed the cyberthreat e-mail service, even though it stated that it "will integrate very closely" with existing entities such as the ISACs. In response, Suzanne Gorman, chair of the financial services sector's ISAC and head of the ISAC Council, stated "we talk about partnerships, but it would have been really nice if they had a conversation with us ahead of making this announcement."[19] As a result, many of the private sector leaders responsible for sharing information about particular critical infrastructure sectors are not sure what new capabilities the alert system will offer, what is expected of them, or how DHS intends to integrate existing networks and private sector efforts into its plans.[20]

Philip Reitinger, Senior Security Strategist for Microsoft, testified to the House Select Committee on Homeland Security on July 15, 2003 that "without a multidisciplinary effort by both

---

[16] U.S. Department of Homeland Security, "U.S. Department of Homeland Security Improves America's Cyber Security Preparedness--Unveils National Cyber Alert System," press release, January 28, 2004, http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0337.xml.
[17] National Infrastructure Protection Center, http://www.nipc.gov/cybernotes/cybernotes.htm.
[18] Michael Mimoso, "Where's the value in DHS' new alert system?" *Searchsecurity.com*, February 2, 2004, *http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci947369,00.html*.
[19] Dan Verton, "New DHS Cyber Alert System Under Fire," *Computerworld*, February 6, 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,89550,00.html.
[20] Ibid.

government and industry, we will not succeed" in protecting our cyber networks.[21] The Administration should improve its efforts to build a private-public partnership for securing cyberspace.

If a crisis were to occur, our nation would need structures and processes in place for real-time coordination among both the private and public sector. The United States does not have these structures in place, and private sector owners and operators of major critical infrastructures are not adequately engaged in efforts that will require numerous entities –within and outside the government – to respond.

SECURITY RECOMMENDATION

The challenges of protecting our critical networks and critical infrastructures require a new paradigm of government and industry leadership for addressing crises as they emerge. The Administration should take several actions if we are to avoid a cyber "9-11."

First, the NCSD Director should have more authority and should report directly to Secretary Ridge or, alternatively, to the President to ensure that we are moving forward on the country's cybersecurity efforts. Second, the Administration should move more rapidly to implement the National Strategy on Cyberspace. Finally, the Administration should create a National Crisis Coordination Center that could house within a single physical facility critical infrastructure representatives from the private sector and federal, state and local government agencies. This center would bring all the relevant parties together in the event of a cyber "9-11."

SECURITY GAP: Government Networks Are Insecure.

Despite the growing threat of cyber attacks, government computer networks remain unprotected. In 1998, Presidential Decision Directive 63 required the federal government to reduce its exposure to threats and serve as a model on how to protect infrastructures. Five years later, this mandate remains unmet. Every year, the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census grades federal agencies on their cybersecurity practices in a "Computer Security Report Card." In December 2003, eight of the agencies surveyed received a failing grade on the security of their computer network systems.[22] The grades were based on information contained in the agencies' Federal Information Security Management Act (FISMA) reports to the Office of Management and Budget for fiscal year 2003.

Agencies receiving failing grades included DHS, Justice, Energy, and State – agencies that play critical roles in the protection of our homeland. Indeed, DHS, which houses the NCSD and is responsible for leading our nation's cybersecurity efforts, received the worst score of any agency – 34 out of 100.

---

[21] U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Industry Speaks* Hearing, July 15, 2003.

[22] U.S. House, Committee on Government Reform, *2003 Federal Computer Security Report Card*, http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652 .

In FISMA, Congress provided federal agencies a framework for securing our computer network systems. Despite this framework, the government's computer networks largely remain insecure. One reason for this is that the government, overall, is not yet requiring vendors to deliver safe systems "out of the box" and ensuring that patches are delivered automatically.[23] Agencies demanding more secure products from vendors will help create more secure software and hardware.[24] When government agencies begin to require their vendors to comply with basic security needs, software and hardware producers will have a market incentive to produce more secure products.

In December 2003, DHS attempted to address the failure of the government to secure its computers by creating the Chief Information Security Officers Forum (CISO Forum) to "share information about programs that are successful and ones that are challenged and need assistance." Under FISMA, each agency must designate a "senior agency information security officer" to coordinate the agency's required security obligations. The Forum would bring these individuals together periodically and on a volunteer basis to share their experiences with cybersecurity within their respective agencies. While the creation of the Forum is commendable, it simply is not enough. The government lacks a single individual who serves as the U.S. government's Chief Security Officer (CSO) to ensure that the various agency CISOs are taking actions and improving the government's cybersecurity.

As long as critical government networks remain unprotected, our homeland security is at risk.

SECURITY RECOMMENDATION

The government should use its procurement power to demand secure products from vendors. Specifically, all government agencies should be required to follow the lead of the Department of Energy, which recently entered into a contract with Oracle requiring the company to deliver its database software preconfigured with the highest level security settings.[25] In addition, the government should strengthen FISMA's security requirements for each agency by using a set of comprehensive collaborative benchmarks for procuring products that are "secure out of the box."

In addition, more and more companies are recognizing the need for company-wide CSOs as part of their leadership. According to the Gartner research firm, fifty percent of Global 2000 companies will have a CSO in place to handle information security by next year.[26] The Administration should create a Federal CSO within the Office of Electronic Government and Information Technology at the Office of Management and Budget who would be accountable and responsible for protecting government computers and developing solid programs throughout the

(Continued on following page)

[23] U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Cybersecurity –Growing Risk from Growing Vulnerability* hearing, June 25, 2003.
[24] Dan Verton, "Some See Hope Beyond Low Government Cybersecurity Grades," *Computerworld*, December 11, 2003, http://www.computerworld.com/securitytopics/security/story/0,10801,88088,00.html?from=imuheads.
[25] Brian Krebs, "Energy Dept. Takes Lead in Security Experiment," *Washington Post*, September 23, 2003, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A53958-2003Sep23&notFound=true.
[26] Joel Strauch,"Spelling out the Chief Security Officer," *Talent Economy Magazine*, October 2003, http://www.talenteconomymag.com/include/article2.php?articleID=280.

government, as well as ensuring that the various federal agencies are complying with FISMA. This official would also determine which benchmarks are appropriate for agencies to use and oversee efforts to assist agencies in procuring products with greater security.

SECURITY GAP: "Cyber First-Responders" Lack Training and Education.

System administrators at companies across the globe are the first protectors and responders of the cybersecurity realm. Unfortunately, the private sector and government have found it difficult to find qualified workers for information security positions.[27] The challenge of providing specialized training for both technology professionals and home computer users extends to all levels of higher education and is especially relevant for those who provide supplementary training for those already in the workforce.[28]

According to the CERT Coordination Center, more than 95 percent of all known computer intrusions can be traced to known vulnerabilities and configuration errors. While "patches" are regularly made available by software and hardware vendors as vulnerabilities are discovered, many system administrators do not regularly apply patches unless there is a crisis or if a "fix" is deemed critical. The Blaster worm this past summer serves as a good example of this problem. Although Microsoft made available a patch to fix the flaw underlying the worm in July 2003, many users failed to install it on their computers, leaving them vulnerable. By August 2003, someone had created the Blaster worm to take advantage of the flaw. Within days of the worm being released, it had infected almost half a million computers.[29] A trained and educated technical workforce is critical to alleviating this quick spreading of viruses and worms.

SECURITY RECOMMENDATION

In furtherance of the development of a culture of security in which all citizens are active contributors, the Administration should earmark funds for developing programs and regional laboratories at universities, colleges, and community colleges to educate information technology professionals about cybersecurity. These academic institutions are the ones that serve their regional workforces and can quickly develop relevant programs and curricula based on their ties with local businesses.[30] For example, the student bodies of community colleges include first-generation college students, and workers seeking further education or training for new careers. As such, these institutions are also in the best position to develop a culture of security within their communities to ensure that all citizens are part of the plan to defend our homeland.

---

[27] National Science Foundation and American Association of Community Colleges, *Cybersecurity Education: The Role of Community Colleges in Protecting Information*, June 2002, http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cyberreport.pdf.

[28] Ibid.

[29] Michelle Delio, "Blaster Worm Still Making Mayhem," www.wired.com, August 30, 2003.

[30] National Science Foundation and American Association of Community Colleges, *Cybersecurity Education: The Role of Community Colleges in Protecting Information*, June 2002, http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cyberreport.pdf.

SECURITY GAP: Individual Users are Being Left Behind As Weak Links In the Battle To Secure Our Computer Networks.

While there have been some efforts, including DHS' creation of cyber bulletins for consumers, to educate home users about cybersecurity, much more needs to be done if we are to secure the weakest links in our computer networks. Since any computer can be used as a point of attack, if individual users do not secure their home systems properly and take an active role in cybersecurity defense, our nation's computers as a whole are vulnerable.[31] Of particular concern is the possibility that thousands of home users' computers have been taken over without their owners' knowledge and will be used to launch "distributed denial of service attacks" (DDoS attacks) against critical computer networks.[32] A DDoS attack occurs when an individual gains control over other people's computers, often through computer viruses, and then uses those computers to send a flood of requests to a particular computer network until it becomes overwhelmed and stops functioning.

The infected computers are often called "zombies," and there are estimates that at any given time thousands of individual users' computers are zombies. The most well-known DDoS attack, orchestrated by a fifteen-year old Canadian calling himself "MafiaBoy," occurred in 2000 and caused more than a billion dollars in damages by shutting down several major Internet sites for a week.[33] It is well-documented that a terrorist organization could use DDoS attacks to compromise key technology systems – such as emergency-response 911 systems or communications systems of first responders – to amplify the consequences of a physical attack.[34]

In addition, the failure of individuals to implement security on new technologies such as broadband and wireless networks is leaving networks insecure. The term "broadband" refers to Internet access that is high-speed and constantly connected to the Internet and includes cable and Digital Subscriber Line (DSL) service. Unfortunately, if users using broadband do not use firewalls and antiviral programs they are at risk, especially since these services often are "always on."

Home users are also installing wireless networks at a staggering pace. The number of U.S. households with wireless networks is believed to have doubled from 3.1 million in 2002 to over six million last year.[35] A number of these networks are unprotected and vulnerable to hackers. The remote nature of wireless networks makes them vulnerable to denial of service attacks. For example, a terrorist could block an entire radio communication channel by transmitting "junk" on certain frequencies, thereby tying up that channel. Bad actors can also "piggyback" on legitimate business and home wireless networks, illegally using those networks to anonymously commit crimes or acts of terror. In many cities, individuals are engaging in "warchalking," where they look for open computer networks and make chalk marks on sidewalks or building walls or post the information on websites so that other computer users can easily find open networks.

---

[31] Cynthia Webb, "Security is in the Hand of the Users," *Washington Post*, August 13, 2003, http://www.washingtonpost.com/wp-dyn/articles/A53577-2003Aug13.html

[32] Dennis Fisher, "Thwarting the Zombies," *e-week*, March 31, 2003, http://www.eweek.com/article2/0,3959,985389,00.asp.

[33] "Mafiaboy Sentenced to 8 Months," *Wired News*, September 13, 2001, http://www.wired.com/news/business/0,1367,46791,00.html.

[34] National Research Council of the National Academies, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*," (Washington DC, 2003).

[35] Jonathan Krim, "WiFi Is Open, Free and Vulnerable to Hackers," *Washington Post*, July 27, 2003, A01.

SECURITY RECOMMENDATION

We should make sure that our citizens are not the "weak links" in today's interconnected and networked environment. If computer networks and systems are to be adequately protected, we should "create cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities," as Tatiana Gau of America Online testified during a Congressional hearing.[36] The government should work more closely with the private sector in developing awareness among our citizenry regarding the necessity of all Americans to protect their part of cyberspace. Specifically, the government and the private sector should establish a framework specifying the actions and best practices that government, Internet service providers, software and hardware vendors, and others should utilize to ensure that individual users are not left behind.

SECURITY GAP: Research and Development Efforts Lag.

There is a need for research and development focusing on preventing, responding, detecting, mitigating, and recovering from cyber attacks. "It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data," testified Richard Perthia, the Director of the Carnegie Mellon CERT Center & Software Engineering Institute during a hearing before the House Select Committee on Homeland Security.[37]

According to the Institute for Information Infrastructure Protection, a consortium of twenty-three academic and not-for-profit research organizations focused on cybersecurity, additional research is needed in several areas including enterprise security management, response and recovery efforts, identification mechanisms, forensics, analysis of security properties and vulnerabilities, trust and authentication, wireless, metrics, legal, policy, and economic issues.[38] Research and development in these areas will help better understand the weaknesses of our networks and systems and how to build stronger networks.

In November 2002, Congress took the important step of passing H.R. 3394, the Cyber Security Research and Development Act, which earmarked federal funds for cybersecurity research and development.[39] The Act authorized $903 million over five years to the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to ensure that the U.S. is better prepared to prevent and combat terrorist attacks on private and government computers. Unfortunately, the Administration continues to request fewer funds than those authorized by the Act. For Fiscal Year 2005, the President's budget only requested $76 million for the NSF and $18.5 million for NIST. These totals are well below the $128.25 million and $61.4 million authorized for NSF and NIST, respectively, in the Act.

---

[36] U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Industry Speaks* hearing, July 15, 2003.
[37] U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Cybersecurity –Growing Risk from Growing Vulnerability* hearing, June 25, 2003.
[38] The Institute for Information Infrastructure Protection, *Cybersecurity Research And Development Agenda*, January 2003, http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf.
[39] U.S. House, Committee on Science, *Summary of H.R. 3394*, http://www.house.gov/science/hot/homeland/cybersum.htm.

In May 2003, the DHS Science & Technology Directorate at DHS of Homeland Security announced it was creating a "Cyber Security Research & Development Center" to work with NSF and NIST on cybersecurity research and development.[40] In early December, DHS announced that the Science & Technology Directorate planned to hire a program manager to help create the cybersecurity expert center.[41] It currently has only a cybersecurity Research & Development director and a contractor working on cybersecurity research issues. Despite the Center and personnel announcements, it is unclear how much the Science & Technology Directorate will be able to accomplish with regards to cybersecurity as it has designated less than two percent of its budget specifically for cybersecurity research and development.[42] For Fiscal Year 2005, the President's budget has only requested $18 million for cybersecurity research and development, a zero increase from the amount appropriated in Fiscal Year 2004 for cybersecurity research in the Science & Technology Directorate. If our country is to have a robust homeland security agenda relating to cybersecurity, the Administration should dedicate more resources to this effort.

SECURITY RECOMMENDATION

The Administration should provide adequate support and resources to the agencies tasked with the government's cybersecurity research and development efforts, as well as provide funding to academia to develop cybersecurity programs and technologies that can be shared among government, universities, and the private sector. Research and development efforts should focus on all aspects of cybersecurity – prevention, detection, and response. To that effect, the Administration and Congress should fund the NSF and NIST at the Fiscal Year 2005 levels specified by Congress in the Cyber Security Research and Development Act.

---

[40] U.S. Department of Homeland Security, *Testimony of Dr. Charles McQueary, Under Secretary, Science and Technology Directorate Before the Committee on Science, U.S. House of Representatives*, May 14, 2003.

[41] Ted Leventhal and Greta Wodele, "Homeland Security science division will also tackle cybersecurity," *govexec.com*, December 4, 2003, http://www.govexec.com/dailyfed/1203/120403tdpm2.htm

[42] U.S. House, Committee on Science, *Hearing Charter: Cybersecurity Research and Development*, May 14, 2003.